IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

JOHN DOE[1], individually and on behalf of all others similarly situated, Plaintiff, v. GATEWAY REHABILITATION CENTER, Defendant.	Case No.: 2:23-cv-93 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff John Doe ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action against Defendant Gateway Rehabilitation Center ("Defendant") and alleges as follows:

JURISDICTION AND VENUE

1. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are members of the proposed Class who are diverse from Defendant, and (4) there are more than 100 proposed Class members.

2. This Court has general personal jurisdiction over Defendant because Defendant is a resident and citizen of this district, Defendant conducts substantial business in this district, and the events giving rise to Plaintiff's claims arise out of Defendant's contacts with this district.

[1] Plaintiff respectfully intends to proceed under a pseudonym in public filings so as not to compound the loss of privacy already suffered. Plaintiff will file a motion to proceed under a pseudonym after conferring with Defendant's counsel to determine if the motion will be opposed. Plaintiff does not object to sharing their identity with the Court or opposing counsel.

3. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) & (2) because Defendant is a resident and citizen of this district and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this district.

PARTIES

4. Plaintiff John Doe is a resident and citizen of Pennsylvania.

5. Defendant Gateway Rehabilitation Center is a Pennsylvania nonprofit corporation with its principal place of business in Moon Township, Pennsylvania.

FACTUAL ALLEGATIONS

I. Gateway Rehabilitation Center

6. Defendant is a provider of drug and alcohol rehabilitation services that operates in Western Pennsylvania.[2]

7. Defendant's patients, like Plaintiff and Class members, provided certain Personal Identifying Information ("PII") and Protected Health Information ("PHI") to Defendant, which is necessary to obtain medical treatment.

8. As a sophisticated rehabilitation services provider with an acute interest in maintaining the confidentiality of the PII and PHI entrusted to it, Defendant is well-aware of the numerous data breaches that have occurred throughout the United States and its responsibility for safeguarding PII and PHI in its possession.

9. Defendant represents to consumers and the public that it possesses robust security features to protect PII and PHI and that it takes its responsibility to protect PII and PHI seriously.[3]

[2] https://www.gatewayrehab.org/locations
[3] https://www.treatspace.com/company/security-and-terms/security-policy/; https://www.treatspace.com/company/security-and-terms/hippa-privacy-policy-statement; https://www.treatspace.com/company/security-and-terms/privacy-policy

II. The Data Breach

10. According to Defendant, on June 13, 2022, Defendant "discovered that it had experienced an incident disrupting access to certain of its systems."[4]

11. Defendant launched an investigation and engaged independent digital forensics and incident response experts.[5]

12. The investigation "confirmed on July 8, 2022 that data potentially containing personal and/or protected health information may have been impacted, and began a comprehensive review process to discern the exact nature of the information and the individuals involved. That review concluded on September 21, 2022 and confirmed that certain personal and/or protected health information of Gateway Rehab current and former patients may have been in the data that was compromised."[6]

13. "The following information may have been involved in the incident: name, date of birth, Social Security number, driver's license or state ID number, financial account and/or payment card number, medical information and health insurance information."[7]

14. Approximately 130,000 patients were affected by the breach.[8]

15. Defendant notified affected patients on November 18, 2022.

16. Defendant sent a letter to Plaintiff dated November 18, 2022, notifying them of the breach. *See* Exhibit A.

---

[4] https://storage.googleapis.com/treatspace-prod-media/pracf/u-2548/Gateway_Rehab_-_Substitute_Notice_-_For_Web_Only.pdf
[5] *Id.*
[6] *Id.*
[7] *Id.*
[8] https://apps.web.maine.gov/online/aeviewer/ME/40/b112c946-f278-49f7-9317-e44880da762e.shtml

17. Defendant's letter also offered free credit monitoring services to those potentially impacted by the breach.

18. Defendant did not state why they were unable to prevent the Data Breach or which security feature failed.

19. Defendant did not state why it did not contact patients about the breach until over five months after discovering the breach or nearly two months after concluding its investigation.

20. Defendant failed to prevent the data breach because it did not adhere to commonly accepted security standards and failed to detect that its databases were subject to a security breach.

III. Injuries to Plaintiff and the Class

21. As a direct and proximate result of Defendant's actions and omissions in failing to protect Plaintiff's PII and PHI, Plaintiff and the Class have been damaged.

22. Plaintiff and the Class have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages, including spending substantial amounts of time monitoring accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud.

23. In addition to the irreparable damage that may result from the theft of PII and PHI, identity theft victims must spend numerous hours and their own money repairing the impacts caused by this breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[9]

24. In addition to fraudulent charges and damage to their credit, Plaintiff and the Class will spend substantial time and expense (a) monitoring their accounts to identify fraudulent or

[9] U.S. Dep't of Justice, *Victims of Identity Theft, 2014* (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

25. Additionally, Plaintiff and the Class have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their PII and PHI is used, the diminution in the value and/or use of their PII and PHI entrusted to Defendant, and loss of privacy.

26. The loss of privacy in this case has caused substantial damage to Plaintiff and the Class because it is now in the public domain that they have sought treatment for substance abuse.

IV. The Value of PII and PHI

27. It is well known that PII and PHI, and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

28. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[10]

29. People place a high value not only on their PII and PHI, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[11]

---

[10] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.

[11] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.

30. People are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[12] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."[13]

31. The PII and PHI of minors can be used to receive illicit gains through methods such as credit card fraud with newly created accounts. The fact that a minor's social security number has not yet been used for financial purposes actually makes it more valued by hackers rather than less. The "blank slate" credit file of a child is much less limited than the potentially low credit score of an adult. Social security numbers that have never been used for financial purposes are uniquely valuable as thieves can pair them with any name and birthdate. After that happens, thieves can open illicit credit cards or even sign up for government benefits.[14]

V. Industry Standards for Data Security

32. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, Deloitte, Equifax, and Capital One, Defendant is, or reasonably

[12] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html.
[13] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf.
[14] Richard Power, "Child Identity Theft: New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers," Carnegie Mellon CyLab, https://www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf.

should have been, aware of the importance of safeguarding PII and PHI, as well as of the foreseeable consequences of its systems being breached.

33. Security standards commonly accepted among businesses that store PII and PHI using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII and PHI;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

34. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[15] and protection of PII and PHI[16] which includes basic security standards applicable to all types of businesses.

35. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

[15] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[16] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

36. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C.

§ 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[17]

37. Because Defendant was entrusted with consumers' PII and PHI, it had, and has, a duty to consumers to keep their PII and PHI secure.

38. Consumers, such as Plaintiff and the Class, reasonably expect that when they provide PII and PHI to Defendant, it will safeguard their PII and PHI.

39. Nonetheless, Defendant failed to prevent the data breach discussed below. Had Defendant properly maintained and adequately protected its systems, it could have prevented the data breach.

VI. HIPAA Standards and Violations

40. In addition to failing to follow universal data security practices, Defendant failed to follow healthcare industry standard security practices, including:

a. Failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. 164.306(a)(2);

b. Failing to ensure compliance with HIPAA security standards by their workforce or agents in violation of 45 C.F.R 164.306(a)(94);

c. Failing to effectively train all members of its workforce and its agents on the policies and procedures with respect to PHI as necessary to maintain the security of PHI in violation of C.F.R. 164.530(b) and 45 C.F.R. 164.308(a)(5); and

[17] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

d. Failing to design and implement and enforce policies and procedures to establish administrative safeguards to reasonably safeguard PHI in compliance with 45 C.F.R. 164.530(c).

CLASS ACTION ALLEGATIONS

41. Plaintiff, individually and on behalf of all others, bring this class action pursuant to Fed. R. Civ. P. 23.

42. The proposed Class is defined as follows:

> **Nationwide Class:** All persons whose PII and PHI was maintained on Defendant's servers that were compromised in the Data Breach.

43. Plaintiff reserves the right to modify, change, or expand the definitions of the proposed Class based upon discovery and further investigation.

44. *Numerosity*: The proposed Class is so numerous that joinder of all members is impracticable. Although the precise number is not yet known to Plaintiff, Defendant has reported that the number of persons affected by the data breach is 130,000.[18] The Class Members can be readily identified through Defendant's records.

45. *Commonality*: Questions of law or fact common to the Class include, without limitation:

a. Whether Defendant owed a duty or duties to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and obtaining their PII and PHI;

b. Whether Defendant breached that duty or those duties;

c. Whether Defendant failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

[18] https://apps.web.maine.gov/online/aeviewer/ME/40/b112c946-f278-49f7-9317-e44880da762e.shtml

d. Whether the security provided by Defendant was satisfactory to protect customer information as compared to industry standards;

e. Whether Defendant misrepresented or failed to provide adequate information to customers regarding the type of security practices used;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and the Class's PII and PHI secure and prevent loss or misuse of that PII and PHI;

g. Whether Defendant acted negligently in connection with the monitoring and protecting of Plaintiff's and Class's PII and PHI;

h. Whether Defendant's conduct was intentional, willful, or negligent;

i. Whether Defendant violated any and all statutes and/or common law listed herein;

j. Whether the Class suffered damages as a result of Defendant's conduct, omissions, or misrepresentations; and

k. Whether the Class is entitled to injunctive, declarative, and monetary relief as a result of Defendant's conduct.

46. *Typicality*: The claims or defenses of Plaintiff are typical of the claims or defenses of the Class. Class members were injured and suffered damages in substantially the same manner as Plaintiff, Class members have the same claims against Defendant relating to the same course of conduct, and Class members are entitled to relief under the same legal theories asserted by Plaintiff.

47. *Adequacy*: Plaintiff will fairly and adequately protect the interests of the proposed Class and has no interests antagonistic to those of the proposed Class. Plaintiff have retained counsel experienced in the prosecution of complex class actions including, but not limited to, data breaches.

48. *Predominance*: Questions of law or fact common to proposed Class members predominate over any questions affecting only individual members. Common questions such as

whether Defendant owed a duty to Plaintiff and the Class and whether Defendant breached its duties predominate over individual questions such as measurement of economic damages.

49. *Superiority*: A class action is superior to other available methods for the fair and efficient adjudication of these claims because individual joinder of the claims of the Class is impracticable. Many members of the Class are without the financial resources necessary to pursue this matter. Even if some members of the Class could afford to litigate their claims separately, such a result would be unduly burdensome to the courts in which the individualized cases would proceed. Individual litigation increases the time and expense of resolving a common dispute concerning Defendant's actions toward an entire group of individuals. Class action procedures allow for far fewer management difficulties in matters of this type and provide the unique benefits of unitary adjudication, economies of scale, and comprehensive supervision over the entire controversy by a single judge in a single court.

50. *Manageability*: Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

51. The Class may be certified pursuant to Rule 23(b)(2) because Defendant has acted on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

52. The Class may also be certified pursuant to Rule 23(b)(3) because questions of law and fact common to the Class will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and efficiently adjudicating the controversy and causes of action described in this Complaint.

53. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(on behalf of the Class)

54. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

55. Defendant owed a duty of care to Plaintiff and Class members to use reasonable means to secure and safeguard the entrusted PII and PHI, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems. These common law duties existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class members would be harmed by the failure to protect their PII and PHI because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendant knew that it was more likely than not Plaintiff and Class members would be harmed by such exposure of their PII and PHI.

56. Defendant's duties to use reasonable security measures also arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and Class members, on the other hand. The special relationship arose because Plaintiff and Class members entrusted Defendant with their PII and PHI, Defendant accepted and held the PII and PHI, and Defendant represented that the PII and PHI would be kept secure pursuant to its data security policies. Defendant alone could have ensured that its data security systems and practices were sufficient to prevent or minimize the data breach.

57. Defendant's duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII and PHI. Various FTC publications and data security breach orders further form the basis of Defendant's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

58. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

59. Defendant breached the aforementioned duties when it failed to use security practices that would protect the PII and PHI provided to it by Plaintiff and Class members, thus resulting in unauthorized third-party access to the Plaintiff's and Class members' PII and PHI.

60. Defendant further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiff's and Class members' PII and PHI within its possession, custody, and control.

61. As a direct and proximate cause of failing to use appropriate security practices, Plaintiff's and Class members' PII and PHI was disseminated and made available to unauthorized third parties.

62. Defendant admitted that Plaintiff's and Class members' PII and PHI was wrongfully disclosed as a result of the breach.

63. The breach caused direct and substantial damages to Plaintiff and Class members, as well as the possibility of future and imminent harm through the dissemination of their PII and PHI and the greatly enhanced risk of credit fraud or identity theft.

64. By engaging in the forgoing acts and omissions, Defendant committed the common law tort of negligence. For all the reasons stated above, Defendant's conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately protect the PII and PHI; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class members' PII and PHI.

65. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII and PHI would not have been compromised.

66. Neither Plaintiff nor the Class contributed to the breach or subsequent misuse of their PII and PHI as described in this Complaint. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and the Class have been put at an increased risk of credit fraud or identity theft, and Defendant has an obligation to mitigate damages by providing adequate credit and identity monitoring services. Defendant is liable to Plaintiff and the Class for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of one year. Defendant is also liable to Plaintiff and the Class to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their PII and PHI, including the amount of time Plaintiff and the Class have spent and will continue to spend as a result of Defendant's negligence. Defendant is also liable to Plaintiff and the Class to the extent their PII and PHI has been diminished in value because Plaintiff and the Class no longer control their PII and PHI and to whom it is disseminated.

COUNT II
INVASION OF PRIVACY
(on behalf of the Class)

67. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

68. Plaintiff and Class members have objective reasonable expectations of solitude and seclusion in their personal and private information and the confidentiality of the content of personal information and non-public medical information.

69. Defendant invaded Plaintiff's and the Class's right to privacy by allowing the unauthorized access to their PII and PHI and by negligently maintaining the confidentiality of Plaintiff's and the Class's PII and PHI, as set forth above.

70. The intrusion was offensive and objectionable to Plaintiff, the Class, and to a reasonable person of ordinary sensibilities in that Plaintiff's and the Class's PII and PHI was disclosed without prior written authorization from Plaintiff and the Class.

71. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff and the Class provided and disclosed their PII and PHI to Defendant privately with an intention that the PII and PHI would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

72. As a direct and proximate result of Defendant's above acts, Plaintiff's and the Class's PII and PHI was viewed, distributed, and used by persons without prior written authorization and Plaintiff and the Class suffered damages as described herein.

73. Defendant is guilty of oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiff's and the Class's PII and PHI with a willful and conscious disregard of their right to privacy.

74. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiff and the Class great and irreparable injury in that the PII and PHI maintained by Defendant can be viewed, printed, distributed, and used by

unauthorized persons. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff and the Class, and Defendant may freely treat Plaintiff's and the Class's PII and PHI with sub-standard and insufficient protections.

COUNT III
BREACH OF IMPLIED CONTRACT
(on behalf of the Class)

75. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

76. Defendant invited Plaintiff and the Class to provide their PII and PHI to Defendant. As consideration for the benefits Defendant was to administer, Plaintiff and the Class provided their PII and PHI to Defendant. When Plaintiff and the Class provided their PII and PHI to Defendant, they entered into implied contracts by which Defendant agreed to protect their PII and PHI and only use it solely to administer benefits. As part of the offer, Defendant would safeguard the PII and PHI using reasonable or industry-standard means.

77. Accordingly, Plaintiff and the Class accepted Defendant's offer to administer benefits and provided Defendant their PII and PHI.

78. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant. However, Defendant breached the implied contracts by failing to safeguard Plaintiff's and the Class's PII and PHI.

79. The losses and damages Plaintiff and the Class sustained that are described herein were the direct and proximate result of Defendant's breaches of its implied contracts with them. Additionally, because Plaintiff and the Class continue to be parties to the ongoing administration and distribution of benefits under the contracts, and because damages may not provide a complete remedy for the breaches alleged herein, Plaintiff and the Class are therefore entitled to specific

performance of the contracts to ensure data security measures necessary to properly effectuate the contracts maintain the security of their PII and PHI from unlawful exposure.

80. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract, and it is liable to Plaintiff and the Class for associated damages and specific performance.

COUNT IV
BREACH OF FIDUCIARY DUTY
(on behalf of the Class)

81. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

82. As alleged above, Plaintiff and the Class had agreements with Defendant, both express and implied, that required Defendant to keep their PII and PHI confidential.

83. The parties had a fiduciary relationship of trust and confidence such that Plaintiff and the Class relied and depended on Defendant to securely maintain their highly sensitive PII and PHI, and Defendant had a duty of care to safeguard Plaintiff and the Class's PII and PHI.

84. Defendant breached that confidence by disclosing Plaintiff's and the Class's PII and PHI without their authorization and for unnecessary purposes.

85. As a result of the data breach, Plaintiff and the Class suffered damages that were attributable to Defendant's failure to maintain confidence in their PII and PHI.

COUNT V
UNJUST ENRICHMENT
(on behalf of the Class)[19]

86. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

[19] This count is plead in the alternative.

87. Plaintiff and the Class have an interest, both equitable and legal, in their PII and PHI that was conferred upon, collected by, and maintained by Defendant and that was ultimately compromised in the data breach.

88. Defendant, by way of its acts and omissions, knowingly and deliberately enriched itself by saving the costs it reasonably should have expended on security measures to secure Plaintiff's and the Class's PII and PHI.

89. Defendant also understood and appreciated that the PII and PHI pertaining to Plaintiff and the Class was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII and PHI.

90. Instead of providing for a reasonable level of security that would have prevented the breach—as is common practice among companies entrusted with such PII and PHI—Defendant instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and the Class. Nevertheless, Defendant continued to obtain the benefits conferred on it by Plaintiff and the Class. The benefits conferred upon, received, and enjoyed by Defendant were not conferred gratuitously, and it would be inequitable and unjust for Defendant to retain these benefits.

91. Plaintiff and the Class, on the other hand, suffered as a direct and proximate result. As a result of Defendant's decision to profit rather than provide requisite security, and the resulting breach disclosing Plaintiff's and the Class's PII and PHI, Plaintiff and the Class suffered and continue to suffer considerable injuries in the forms of, *inter alia*, attempted identity theft, time and expenses mitigating harms, diminished value of PII and PHI, loss of privacy, and increased risk of harm.

92. Thus, Defendant engaged in opportunistic conduct in spite of its duties to Plaintiff and the Class, wherein it profited from interference with Plaintiff's and the Class's legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its conduct.

93. Accordingly, Plaintiff, on behalf of himself and the Class, respectfully requests that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically, the amounts that Defendant should have spent to provide reasonable and adequate data security to protect Plaintiff's and the Class's PII and PHI, and/or compensatory damages.

COUNT VI
BAILMENT
(on behalf of the Class)

94. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

95. Plaintiff and the Class provided, or authorized disclosure of, their PII and PHI to Defendant.

96. In allowing their PII and PHI to be made available to Defendant, Plaintiff and the Class intended and understood that Defendant would adequately safeguard their PII and PHI.

97. For its own benefit, Defendant accepted possession of Plaintiff's and the Class's PII and PHI.

98. By accepting possession of Plaintiff's and the Class's PII and PHI, Defendant understood that Plaintiff and the Class expected Defendant to adequately safeguard their PII and PHI. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties. During the bailment (or deposit), Defendant owed a duty to Plaintiff and the Class to exercise reasonable care, diligence, and prudence in protecting their personal information.

99. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and the Class's personal information, resulting in the unlawful and unauthorized access to and misuse of their PII and PHI.

100. As a direct and proximate result of Defendant's breach of its duty, Plaintiff and Class Members suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth above.

101. As a direct and proximate result of Defendant's breach of its duties, the personal information of Plaintiff and the Class entrusted, directly or indirectly, to Defendant during the bailment (or deposit) was damaged and its value diminished.

COUNT VII
VIOLATION OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW
73 P.S. 201-1 *et seq.*
(on behalf of the Class)

102. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

103. Defendant is a "person" as defined by 73 P.S. § 201-2(2).

104. Plaintiff and Class members purchased goods and services in "trade" and "commerce" as defined by 73 P.S. § 201-2(3).

105. Defendant engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 P.S. § 201-3, including the following:

a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 P.S. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 P.S. § 201- 2(4)(vii)); and

c. Advertising its goods and services with intent not to sell them as advertised (73 P.S. § 201-2(4)(ix)).

d. Defendant's unfair or deceptive acts and practices include:

e. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members' Personal Information, which was a direct and proximate cause of the Breach;

f. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Breach;

g. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

h. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Class members' Personal Information, including by implementing and maintaining reasonable security measures;

i. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

j. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Class members' Personal Information; and

k. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff

and Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

106. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' PII and PHI.

107. Defendant intended to mislead Plaintiff and Class members and induce them to rely on its misrepresentations and omissions.

108. Had Defendant disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant held itself out as secure and was trusted with sensitive and valuable PII and PHI regarding customers, including Plaintiff and the Class.

109. Defendant accepted the responsibility of being a "steward of data" while keeping the inadequate state of its security controls secret from the public.

110. Plaintiff and the Class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

111. Defendant acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Class members' rights. Past data breaches across the industry put Defendant it on notice that its security and privacy protections were needed to be investigated and were likely inadequate.

112. As a direct and proximate result of Defendant's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff and the Class members' reliance on them, Plaintiff and Class members have suffered and will continue to suffer injury, ascertainable losses

of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII and PHI.

113. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays for a judgment against Defendant as follows:

a. For an order certifying the proposed Class, appointing Plaintiff as Representative of the proposed Class, and appointing the law firms representing Plaintiff as counsel for the Class;

b. For compensatory and punitive and treble damages in an amount to be determined at trial;

c. Payment of costs and expenses of suit herein incurred;

d. Both pre-and post-judgment interest on any amounts awarded;

e. Payment of reasonable attorneys' fees and expert fees;

f. Such other and further relief as the Court may deem proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial by jury.

Dated: January 18, 2023

Respectfully submitted,

/s/ Charles E. Schaffer
Charles E. Schaffer
Nicholas J. Elia
LEVIN, SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Phone: (215) 592-1500
cschaffer@lfsblaw.com
nelia@lfsblaw.com

Jeffrey S. Goldenberg
Todd B. Naylor
Robert B. Sherwood
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Phone: (513) 345-8291
Facsimile: (513) 345-8294
jgoldenberg@gs-legal.com
tnaylor@gs-legal.com
rsherwood@gs-legal.com

Counsel for Plaintiff and Proposed Class